۱

امنیت اطلاعات در شبکه‌های صنعتی

IT Security VS OT Security

چگونه شبکه‌های صنعتی را در برابر تهدیدات سایبری ایمن کنیم؟

برسام
برنامه‌سازمانی آگاهی‌رسانی امنیت سایبری شرکت تولید نیروی برق حرارتی

پژوهشگاه نیرو

شرکت مادر تخصصی تولید نیروی برق حرارتی

۶

در دنیای امروز
حفظ امنیت سایبری
دیگر یک انتخاب نیست، یک الزام است.

درباره چیزهایی که خواندید، اگرسوالی داشتید؛ نه تنها خوشحال می‌شویم که بشنویم و پاسخ دهیم، بلکه شما را تشویق می‌کنیم که بیشتر کنجکاوی کنید و بیشتر بپرسید!

کارگروه فرهنگ‌سازی و آگاهی‌رسانی امنیت سایبری
شرکت مادرتخصصی تولید نیروی برق حرارتی
(طرح برسام)
تلفن دبیرخانه کارگروه برسام:
۵۸۳۷۶۶۴۲
پست الکترونیکی کارگروه برسام :
barsam[at]tpph.ir

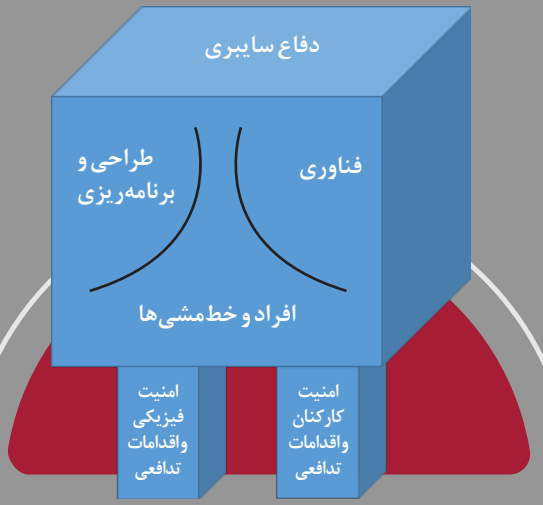
۵

چگونه شبکه‌های صنعتی را در برابر تهدیدات سایبری امن کنیم؟

امنیت، یک فرایند است و چیزی با عنوان امنیت مطلق وجود ندارد. یعنی شبکه‌ای که امروز امن است، شاید فردا ناامن باشد؛ زیرا هکرها همواره به دنبال روش‌های جدید حمله و نفوذ هستند. امن‌سازی شبکه‌های صنعتی نیازمند فناوری است. اما فناوری تنها جزء لازم برای این فرایند نیست. **امن‌سازی موفقیت‌آمیز** ترکیب مناسبی از این اجزا است:

- کاربران آگاه و آموزش‌دیده
- ساختار مناسب سازمانی
- راهبردهای امنیتی متناسب با ساختار سازمانی
- خط‌مشی‌ها و دستورالعمل‌های مؤثر و کارا
- برنامه‌های ارزیابی و ممیزی
- فناوری امنیت سایبری متناسب با موارد فوق در سطحی از پیچیدگی که برای کاربران، قابل فهم باشد.

در فرایند امنیت شبکه، **اجزای دیگری** هم دخیل هستند، شامل: دارایی (از چه چیزی می‌خواهیم محافظت کنیم)، تهدید (فرد یا رویدادی که می‌تواند آسیب‌زا باشد)، تأثیرگذاری (شدت و عواقب آسیبی که می‌تواند رخ دهد)، احتمال (میزان تکرارپذیری تهدید در بازه زمانی مشخص) و اقدامات تدافعی (روش‌هایی برای کاهش ریسک)
ترکیب همه این موارد می‌تواند یک طرح دفاع سایبری خوب برای ما فراهم کند.



۲

آیا واقعاً شبکه‌های صنعتی را رخدادهای سایبری تهدید می‌کنند؟

برای آنکه درباره امنیت شبکه‌های صنعتی صحبت کنیم، لازم است که ابتدا **تعریفی از شبکه صنعتی** ارائه کنیم. بر اساس استاندارد IEC62443 ، سامانه‌های کنترل و اتوماسیون صنعتی عبارت‌اند از: سامانه‌های کنترل کارخانه‌های تولیدی و فرایندی، سامانه‌های کنترل محیطی ساختمان، عملیات گسترده در سطح جغرافیایی مانند تأسیسات (برق، آب، گاز و ...)، خطوط لوله و شبکه‌های توزیع نفت و دیگر صنایع و کاربردهایی نظیر شبکه‌های حمل‌ونقل که از امکانات خودکار نظارتی و کنترلی راه دور بهره می‌برند.

وقتی درباره امنیت شبکه صنعتی صحبت می‌کنیم، درواقع به حوزه در حال گسترشی اشاره می‌کنیم که بیشتر با چگونه امن نگه داشتن شبکه‌های صنعتی و درنتیجه ایمن نگه‌داشتن افراد، فرایندها و تجهیزاتی ارتباط دارد که به آن‌ها وابسته هستند. **امن‌بودن یعنی** عاری‌بودن از آسیب موجود یا احتمالی که می‌تواند خسارت فیزیکی یا سایبری به اجزای شبکه صنعتی وارد کند یا اختلالی در آن به وجود آورد.

به‌عنوان یک مثال، در نظر بگیرید که یک کارمند ناراضی می‌خواهد نارضایتی خود را از طریق ایجاد اختلال در نیروگاه برق تلافی کند. او می‌تواند بدافزاری را روی یکی از سیستم‌ها قرار دهد یا آچاری را بردارد و یکی از نشانگرها را منهدم کند و یا حتی یکی از رک‌ها را با زور بازکند و جامپری را برای از کار انداختن سیستم هشدار صوتی جابه‌جا کند.

طبق تعریف، موارد اول و سوم در حیطه امنیت شبکه صنعتی و مورد دوم در گروه خرابکاری عمدی جای می‌گیرد. با این تعریف و مثال می‌بینیم که **عوامل درون‌سازمانی یا بیرون سازمانی** می‌توانند به شکل‌های مختلف ازجمله انسانی، فرایندی و سایبری، امنیت شبکه صنعتی را تهدید کنند. حالا در نظر بگیرید که شبکه تولید- انتقال- توزیع برق با همه پیچیدگی و اهمیت حیاتی که دارد تا چه حد می‌تواند در معرض انواع آسیب‌پذیری‌های سایبری قرار گیرد.

۳

ارتباط بین امنیت در شبکه‌های فناوری اطلاعات و شبکه‌های صنعتی

تفاوت زیادی بین شبکه‌های مبتنی بر فناوری اطلاعات (IT) و شبکه‌های مبتنی بر عملیات (OT) وجود دارد. در شبکه‌های IT به ترتیب بر مفاهیم محرمانگی، یکپارچگی و دسترسی‌پذیری تأکید می‌شود. حال‌آنکه در شبکه‌های OT، **اولویت اول** با دسترسی‌پذیری و بعد یکپارچگی و محرمانگی است. این روند همان چیزی است که امنیت OT را از امنیت IT متمایز می‌کند. یعنی اگر این توالی رعایت نشود، باکیفیت‌ترین راهکارهای امنیتی نیز کارایی نخواهند داشت و تمامیت سیستم صنعتی در خطر قرار خواهد گرفت.

برای آنکه بتوان به امنیت سایبری در شبکه‌های صنعتی با **رویکردی کل‌نگر** نگریست، لازم است که سه رکن کلیدی را مدنظر داشت: داشتن رویکرد فرایندمحور (Process) نسبت به پیاده‌سازی امنیت، انجام آگاهی‌رسانی و آموزش کارکنان (People) و به‌کارگیری فناوری‌هایی (Technology) که به‌طور خاص برای محیط‌های صنعتی ایجادشده‌اند. یعنی نگاه به امنیت در هر سطحی از شبکه، آموزش و آگاهی‌رسانی امنیتی از بالاترین سطح مدیریت تا نیروهای اجرایی و فناوری و فنی، ایمن‌سازی مستمر در حین محافظت از اطلاعات و فرایندهای فناوری.

به دلیل همین پیچیدگی و چندوجهی بودن راه‌حل امنیت سایبری، حملات سایبری نیز چندلایه و پیچیده هستند و معمولاً مهاجمان برای آسیب‌رسانی به شبکه‌های صنعتی از روش‌های ترکیبی فیزیکی-انسانی-سایبری در حملات استفاده می‌کنند.

۴

مهم‌ترین رخدادهای سایبری در شبکه‌های صنعتی

جولای ۲۰۱۰

استاکس‌نت و کشف حملاتی که به زیرساخت‌های حیاتی ایران و ازجمله سایت‌های هسته‌ای انجام گرفت.

دسامبر ۲۰۱۴

نفوذ به کارخانه فولادسازی آلمان به روش فیشینگ هدف‌دار موجب بروز صدمات فراوانی شد.

دسامبر ۲۰۱۵

خاموشی سراسری برق در غرب اوکراین با نفوذ بدافزار فیشینگ هدف‌دار BlackEnergy

مارس ۲۰۱۶

نفوذگران با سوءاستفاده از یک آسیب‌پذیری در سامانه کنترل تأسیسات تصفیه آب شهر نیویورک توانستند سطح مواد شیمیایی مورداستفاده برای تصفیه آب را تغییر دهند.

ژوئن ۲۰۱۷

باج‌افزار Petya NonPetya/ با حمله به شرکت توزیع برق اوکراین، شرکت Mearsk و برخی دیگر زیرساخت‌های OT آن‌ها را آلوده‌کرد و از کار انداخت.

جولای ۲۰۱۷

کمپین نفوذ به بخش انرژی، بیش از ۱۵ شرکت آمریکایی را هدف قرارداد.

دسامبر ۲۰۱۷

بدافزار Triton، کنترلرهای ایمنی و صنعتی شرکت Triconex که در صنایع زیرساختی کاربری فراوانی دارد را در سطح جهان و به‌ویژه خاورمیانه آلوده کرد.

مارس ۲۰۱۹

خاموشی گسترده و چند نوبته در شبکه برق ونزوئلا به‌سبب حملات سایبری